

5 FAM 860 SYSTEM SECURITY

5 FAM 861 SECURITY PROCEDURES

(TL:IM-14; 12-30-94)

The system manager implements security controls on automated information systems as established by the Bureau of Diplomatic Security (reference 12 FAM). The following are key issues for system managers.

(1) Incorporate user-oriented systems security information into current and future post security training and awareness programs. Emphasize protecting unclassified, sensitive information as well as classified information. A prepared briefing package, including slides and a film, are available from DS/CIS/IST upon request.

(2) Add the ISSO to the post checkout list. The ISSO must promptly remove access privileges of users departing from post.

(3) Prepare written guidance on identifying and handling sensitive unclassified information. Include this information in regularly scheduled awareness briefings.

(4) Perform background checks on the local vendor technicians in the local environment.

(5) Maintain a log of all daily operations.

(6) Install a high-volume shredder to accommodate the destruction of large computer listings.

(7) Periodically browse through word processing files to ensure that sensitive information is adequately protected and that classified information is not being placed on the system.

5 FAM 862 COMPUTER ROOM SECURITY

(TL:IM-14; 12-30-94)

a. Prominently display emergency response instructions inside the computer room.

b. Ensure that DS-approved access control locks are installed and operational on all computer room exterior doors. The combination to the lock should be changed periodically and given to authorized individuals who have a need-to-know.

c. Post an authorized room access list and an emergency contact list at the entrance to the computer room.

d. Whenever feasible, install and clearly identify an emergency power off switch outside the computer room near its entrance.

5 FAM 863 SYSTEM SECURITY

(TL:IM-14; 12-30-94)

The person assigned system management responsibilities should:

(1) Develop, document, implement, and monitor a full volume and data file backup program that includes provisions for storage of backup media and copies of essential or unique operating instructions and manuals at a secure off-site location. Review and match incremental backups against full volume backups before re-using the media.

(2) Develop local procedures for power up/power down, system restart/recovery, and system operating procedures. Post written procedures inside the computer room.

(3) Assign randomly generated alphanumeric passwords to all system users.

(4) Implement a password receipt procedure. Reference 12 FAM for a suggested form.

(5) Store archive diskettes in a secure location after normal working hours.

(6) Restrict users to workstations in their functional areas. Use the system's security program to place restrictions on individual user IDs.

(7) Regularly remind all word processing users that they are never authorized to originate, process and/or store classified information on unclassified automated information systems. The following applies to LOU information.

(a) Store all magnetic media (hard disks, diskettes, tapes, printer ribbons, etc.) containing LOU or administratively controlled information in approved containers and protect in accordance 12 FAM 940 .

(b) Process or store LOU or administratively controlled information only on systems limited to Americans and cleared FSNs.

(c) Do not send systems with non-removable disks approved for the processing of LOU information outside of the embassy for maintenance.

(d) Do not store or process LOU on an unclassified system at high technical threat foreign service posts.

(8) Use encryption as a method of protecting information for transmission through uncontrolled paths. Encryption is the only authorized method of providing suitable system and data protection. A/IM/SO/TO/SI is the controlling office for distributing encryption devices and Digital Encrypting System (DES). Submit all requests to initiate new links transmitting to uncontrolled areas to A/IM/SO/TO/SI and DS/ST/ISS for approval.

(9) Limit system security administrator privileges to computer center staff with a demonstrated need for special access privileges. Issue users randomly generated passwords.

(10) Restrict system access of personnel in sensitive ADP positions until their security checks or background investigations are completed.

(11) Document the condition of all hardware shipments upon receipt at post and examine them for possible tampering.

(12) Ensure that archiving via archiving workstations or personal computers is accomplished under the direct supervision of American supervisors.

(13) Send damaged, removable magnetic storage media containing classified or sensitive data to: A/IM/SO/FO, DPM/C Room B528, Halifax Engineering, Main State. Label the media "For Destruction."

(14) Delete all logon user IDs that are not attributable to a specific individual.

(15) Conduct semiannual reviews of CUE access levels to determine if each system user is appropriately restricted to functions required by the normal duties.

5 FAM 864 THROUGH 869 UNASSIGNED